

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

APR 24 2019

UNITED STATES OF AMERICA

v.

TAL PRIHAR
MICHAEL PHAN
d/b/a DEEPDOTWEB,

Defendants.

Criminal No. 19-115
(18 U.S.C. § 1956(h))
[UNDER SEAL]

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

COUNT ONE

**Conspiracy to Commit Money Laundering
(18 U.S.C. § 1956(h))**

INTRODUCTION

1. At all times material to this Indictment:

- a. TAL PRIHAR was an Israeli citizen residing in Brazil.
- b. MICHAEL PHAN was an Israeli citizen residing in Israel.
- c. From in and around October 2013 and continuing through the date of this

Indictment, TAL PRIHAR and MICHAEL PHAN, the defendants, owned and operated a website known as “DeepDotWeb” (“DDW”), hosted at www.deepdotweb.com and also accessible on the darknet at DeepDot35Wveyd5.onion.

d. DDW provided users with direct access to numerous online darknet marketplaces, not accessible through traditional search engines, at which vendors offered for sale illegal narcotics such as fentanyl, carfentanil, cocaine, heroin, and crystal methamphetamine; firearms, including assault rifles; malicious software and hacking tools; stolen financial information and payment cards and numbers; access device-making equipment; and other illegal contraband.

e. PRIHAR and PHAN received kickback payments, representing a portion of the proceeds from each purchase of the aforementioned illegal goods made by individuals referred to a darknet marketplace from the DDW site. These kickback payments were made in virtual currency, such as bitcoin, and paid into a DDW-controlled bitcoin “wallet.”

f. To conceal and disguise the nature and source of the illegal proceeds, totaling over \$15 million, PRIHAR and PHAN transferred their illegal kickback payments from their DDW bitcoin wallet to other bitcoin accounts and to bank accounts they controlled in the names of shell companies.

g. To maximize purchases made on the darknet marketplaces and their kickbacks from those purchases, DDW featured tutorials on how to buy drugs online through darknet marketplaces and offered comparisons and reviews of various marketplaces. DDW warned users of worldwide law enforcement actions associated with criminal activity on the darknet.

STATUTORY ALLEGATIONS

2. Beginning in and around October 2013, and continuing through the date of this Indictment, in the Western District of Pennsylvania and elsewhere, the defendants, TAL PRIHAR and MICHAEL PHAN, did knowingly, intentionally and unlawfully conspire together with each other, with darknet marketplace administrators, and with other persons known and unknown to the grand jury to commit certain offenses against the United States, that is, to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, (1) with the intent to promote the carrying on of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i), and (2) knowing that the property involved in the transactions represented the

proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

3. It is further alleged that the specified unlawful activity included:

a. the felonious manufacture, importation, receiving, concealment, buying, selling, and otherwise dealing in a controlled substance, in violation of Title 21, United States Code, Sections 846 and 841(a)(1), punishable under the laws of the United States;

b. fraud and related activity in connection with identification documents in violation of Title 18, United States Code, Section 1028;

c. fraud and related activity in connection with access devices in violation of Title 18, United States Code, Section 1029; and

d. fraud and related activity in connection with computers in violation of Title 18, United States Code, Section 1030;

All in violation of Title 18, United States Code, Section 1956(h).

MANNER AND MEANS OF THE CONSPIRACY

Kickback Payments

4. During all times relevant to the Indictment, darknet marketplaces operated on the “Tor” network, a computer network designed to facilitate anonymous communication over the Internet. Because of Tor’s structure, a user who wanted to visit a particular darknet marketplace needed to know the site’s exact .onion address. DDW simplified this process by including pages of hyperlinks to various darknet marketplaces’ .onion addresses.

5. Users who visited DDW were able to click on the hyperlinks to navigate directly to the darknet marketplaces. Embedded in these links were unique account identifiers which enabled the individual marketplaces to pay what they referred to as “Referral Bonuses,” to DDW. Referral bonuses, paid in virtual currency, were a percentage of the profits of all of the activities conducted on the marketplace by any user who made purchases on the marketplace by using DDW’s customized referral link. Through the use of the referral links, DDW received kickbacks from darknet marketplaces every time a purchaser used DDW to buy illegal narcotics or other illegal goods on the marketplace.

6. During the time period relevant to this Indictment, DDW’s referral links were widely used by users in the Western District of Pennsylvania and elsewhere to access and then create accounts on many darknet marketplaces. Over the course of the conspiracy, the defendants referred hundreds of thousands of users to darknet marketplaces. These users in turn completed hundreds of millions’ of dollars’ worth of transactions, including purchases of illegal narcotics such as fentanyl, carfentanil, cocaine, heroin, and crystal methamphetamine; firearms, including assault rifles; malicious software and hacking tools; stolen financial information and payment cards and numbers; access device-making equipment; and other illegal contraband. Through the use of the referral links, the defendants reaped commissions worth millions of dollars, generated from the illicit sales conducted on darknet marketplace accounts created through the site.

7. The defendants grew and promoted the DDW site, which functioned to drive further traffic to the DDW referral links, generating additional income for the defendants. PRIHAR functioned as the administrator of DDW. He registered the domain, made infrastructure payments and maintained control over site content. PHAN was responsible for DDW’s technical operations,

designing and maintaining the website's day-to-day operation. PHAN and PRIHAR communicated on a daily basis to facilitate their criminal enterprise.

8. From in or before November 2014 until the date of this Indictment, the defendants controlled a bitcoin wallet that they used to receive the kickback payments for purchases completed on the various darknet marketplaces. Throughout the course of the conspiracy, DDW operated accounts on darknet markets and communicated with the operators of various darknet markets regarding kickback payments.

Relevant Marketplaces

9. At various times relevant to this Indictment, DDW posted referral links to numerous darknet marketplaces, including: AlphaBay Market, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D's, Wall Street Market, and Tochka Market.

10. AlphaBay Market was a darknet market in operation from December 2014 to July 2017, when the site was seized by law enforcement. At the time of the seizure, AlphaBay was the largest criminal marketplace in operation, offering a vast platform for users to purchase illegal drugs, fraudulent identification materials, counterfeit goods, hacking tools, malware, firearms, and toxic chemicals. Approximately 23.6% of all orders completed on AlphaBay were associated with an account created through a DDW referral link, meaning that DDW received a referral fee for 23.6% of all orders made on AlphaBay.

11. Agora Market was a darknet market in operation from in and about September 2013 to in and around August 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

12. Abraxas Market was a darknet market in operation from in and about January 2015 to in and around November 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

13. Dream Market was a darknet market in operation from in and around November 2013 continuing through the date of this Indictment. Dream Market sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

14. Valhalla Market was a darknet market that was originally established in and around October 2013 under a different name but rebranded itself as Valhalla Market in and around 2015. Valhalla Market continued to operate through the date of this Indictment. Valhalla Market sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

15. Hansa Market was a darknet market in operation from in and around August 2015 to July 2017, when the website was taken offline by law enforcement. Hansa offered tens of thousands of listings of illegal narcotics, including fentanyl, heroin, and cocaine, drug paraphernalia, and counterfeit and fraud-related goods and services, which customers purchased using virtual currencies, including Bitcoin. DDW referred over 198,000 users to Hansa Market, accounting for approximately 47.2% of all of Hansa's users. DDW received a commission on all of those users' purchases.

16. TradeRoute Market was a darknet market in operation from in and around September 2016 to in and around September 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

17. Dr. D's Market was a darknet market in operation from in and around 2015 to in and about 2016 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

18. Wall Street Market was a darknet market that has been in operation from in and around November 2016 continuing through the date of this Indictment. Wall Street Market sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

19. Tochka Market was a darknet market that has been in operation from in and around January 2015 continuing through the date of this Indictment. Tochka Market sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband.

20. During the time period relevant to this Indictment, users located in the Western District of Pennsylvania and elsewhere could and did click on the DDW referral links for the markets above and created accounts with each of the above marketplaces. DDW users used these accounts to purchase illegal narcotics, such as fentanyl, carfentanil, heroin, cocaine, methamphetamine, crystal methamphetamine, MDMA, LSD, OxyContin, oxycodone, hydrocodone, and Xanax; firearms, including assault rifles; hacking tools, such as keyloggers, proxy servers, and virtual private network (VPN) services; fake and stolen identification documents, such as driver's licenses and passports; and stolen access devices, including credit card numbers and hacked accounts for numerous providers, including U.S.-based financial institutions, internet service providers, ridesharing services, and video streaming services. As the owners and operators of DDW, the defendants earned a kickback for every illegal purchase conducted by accounts created via the DDW market referral link.

Specific Illicit Payments

21. Between in and around November 2014 and April 10, 2019, DDW received approximately 8,155 bitcoin in kickback payments from darknet marketplaces, worth approximately \$8,414,173 when adjusted for the trading value of bitcoin at the time of each transaction. This included:

Marketplace	Number of Withdrawal Transactions	Bitcoin	USD Equivalent
AlphaBay	6,147	3,273	\$1,567,913
Agora	2,175	844.6990817	\$220,460.71
Abraxas	211	380.997177	\$97,548.76
Dream	261	99.1503695	\$197,589.12
Hansa	1,124	11.69021541	\$14,791.26
TradeRoute	22	8.441655	\$35,134.39
Dr. D's	25	2.6316	\$659.60
Wall Street	7,755	2.572515	\$18,729.40
Tochka	2,990	0.70483642	\$5,072.33

22. The bitcoin was transferred to DDW's bitcoin wallet, controlled by the defendants, in a series of more than 40,000 deposits and was subsequently withdrawn to various destinations both known and unknown to the grand jury through over 2,700 transactions. Due to bitcoin's fluctuating exchange rate, the value of the bitcoin at the time of the withdrawals from the DDW bitcoin wallet equates to approximately \$15,489,415.

Transactions in the Western District of Pennsylvania

23. Between in and around December 2016 and on or about July 4, 2017, approximately four dozen individuals in the Western District of Pennsylvania used a DDW referral link to create accounts on AlphaBay Market. These users purchased thousands of dollars of illegal narcotics, including crack cocaine and crystal methamphetamine, oxycodone, and LSD, as well as a fake custom passport, which they had shipped to the Western District of Pennsylvania. DDW received a kickback from each purchase made.

24. Between in and around January 2016 and on or about July 18, 2017, approximately 65 individuals in the Western District of Pennsylvania used a DDW referral link to create accounts on Hansa Market. These users purchased illegal narcotics, including cocaine and methamphetamine, oxycodone, and LSD, and fake payroll checks, which they had shipped to the Western District of Pennsylvania, as well as proxy servers. The defendants received a kickback from each purchase made.

25. On September 20, 2017, an FBI undercover employee in the Western District of Pennsylvania purchased 6 grams of crystal methamphetamine from a vendor operating on Tochka Market. A commission from that illegal drug transaction was transferred to DDW's bitcoin wallet.

26. On April 12, 2019, an FBI undercover employee in the Western District of Pennsylvania visited the DDW website and created an account on Tochka Market using the DDW referral link. Using the DDW-linked account, the FBI undercover employee purchased 10 grams of crystal methamphetamine at a cost of \$470.00.

27. On April 16, 2019, an FBI undercover employee in the Western District of Pennsylvania visited the DDW website and created an account on Tochka Market using the DDW

referral link. Using the DDW-linked account, the FBI undercover employee purchased the following items:

- a. 10 grams of crystal methamphetamine at a cost of \$407.72;
- b. 60 OxyContin 60mg tablets at a cost of \$431.66; and
- c. Tricera Ransomware, a software that encrypts victims' computers and renders them useless until a ransom is paid, at a cost of \$82.38.

28. On April 16, 2019, an FBI undercover employee in the Western District of Pennsylvania visited the DDW website and created an account on Wall Street Market using the DDW referral link. Using the DDW-linked account, the FBI undercover employee purchased the following items:

- a. 3.5 grams of heroin at a cost of \$82.38;
- b. 2 compromised credit cards at a cost of \$37.80; and
- c. 10 grams of cocaine at a cost of \$480.00.

Shell Companies and Related Accounts

29. In seeking to conceal their illicit activities and protect their criminal enterprise and the illegal proceeds it generated, the defendants set up numerous shell companies around the world. The defendants used these companies to move their ill-gotten gains and conduct other activity related to DDW. These companies included WwwCom Ltd., M&T Marketing, Imtech, O.T.S.R. Biztech, and Tal Advanced Tech.

30. Throughout the course of the conspiracy, the defendants held numerous accounts at the virtual currency exchanges and related companies to which they routed their ill-gotten gains. These accounts were held in the names of PRIHAR, PHAN, M & T Marketing LTD, WwwCom LTD., and WwCom LTD., an apparent misspelling of WwwCom LTD.

31. The defendants subsequently moved funds into multiple bank accounts, which they controlled, including accounts at Baltikums Bank in Latvia, First International Bank of Israel in Israel, and TBC Bank in Georgia.

In violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATIONS

32. The allegations of this Indictment are re-alleged and by this reference fully incorporated herein for the purpose of alleging criminal forfeiture to the United States of America of certain property in which the defendants, TAL PRIHAR and MICHAEL PHAN, have an interest.

33. As a result of committing the money laundering offense alleged in Count One of this Indictment, the defendants, TAL PRIHAR and MICHAEL PHAN, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in the offense, or any property traceable to such property.

Specific Property

34. The property subject to forfeiture includes, but is not limited to, the following:

a. Virtual currency accounts:

- i. OKCoin (corporate account in the name of Wwwcom LTD);
- ii. Kraken (individual account in the name of TAL PRIHAR);
- iii. BitPay (corporate account in the name of Wwwcom LTD);

b. PayPal.com (account in the name of TAL PRIHAR);

c. Bank accounts:

- i. Baltikums Bank in Latvia, account number LV70 XXXX XXXX XXXX
0001 0;
- ii. TBC Bank in Georgia, account number
GE96TBXXXXXXXXXXXX0004; and
- iii. First International Bank of Israel in Israel, account number
IL2903XXXXXXXXXXXX3723.

Money Judgment

35. The United States will seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, involved in this offense, and any property traceable to such property, of at least approximately \$15,489,415 in United States currency.

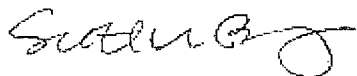
Substitute Assets

36. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (1) cannot be located upon the exercise of due diligence;
- (2) has been transferred or sold to, or deposited with, a third person;
- (3) has been placed beyond the jurisdiction of the Court;
- (4) has been substantially diminished in value; or
- (5) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

All pursuant to Title 18, United States Code, Section 982(a)(1).



SCOTT W. BRADY
United States Attorney
PA ID NO. 88352